

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM  
Internationales Büro



INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE  
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation <sup>6</sup> :

H03K 3/84

A1

(11) Internationale Veröffentlichungsnummer: WO 99/39434

(43) Internationales  
Veröffentlichungsdatum:

5. August 1999 (05.08.99)

(21) Internationales Aktenzeichen: PCT/EP98/08057

(22) Internationales Anmeldedatum: 10. Dezember 1998  
(10.12.98)

(30) Prioritätsdaten:  
198 06 178.1 2. Februar 1998 (02.02.98) DE

(71) Anmelder (für alle Bestimmungsstaaten ausser  
US): DEUTSCHE TELEKOM AG [DE/DE];  
Friedrich-Ebert-Allee 140, D-53113 Bonn (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): DULTZ, Wolfgang  
[DE/DE]; Marienberger Strasse 37, D-65936 Frankfurt  
am Main (DE). DULTZ, Gisela [DE/DE]; Marienberger  
Strasse 37, D-65396 Frankfurt am Main (DE). HILDE-  
BRANDT, Eric [DE/DE]; Ginnheimer Strasse 20, D-60487  
Frankfurt am Main (DE). SCHMITZER, Heidrun [DE/DE];  
König-Philipp-Weg 25, D-93051 Regensburg (DE).

(81) Bestimmungsstaaten: CA, CN, JP, NO, US, europäisches  
Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR,  
IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht

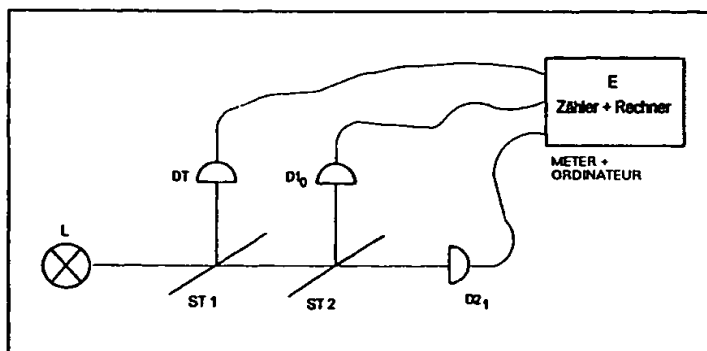
Mit internationalem Recherchenbericht.

(54) Title: METHOD AND ARRANGEMENT FOR GENERATING BINARY SEQUENCES OF RANDOM NUMBERS

(54) Bezeichnung: VERFAHREN UND ANORDNUNG ZUR ERZEUGUNG BINÄRER SEQUENZEN VON ZUFALLSZAHLN

(57) Abstract

The aim of the invention is to provide an inexpensive method and an arrangement for generating binary sequences of random numbers. The invention should also be easy to integrate onto a chip card. The inventive method is based on the principle of the random path selection of photons in a beam splitter and the generation of a random numbers by means of two detectors (D<sub>10</sub>; D<sub>21</sub>) situated downstream of a beam splitter (ST2). According to the invention, a low-power light source (L) is used to produce the photons and an additional beam splitter (ST1) is arranged upstream of the original beam splitter (ST2). The photons emitted by the light source (L) for a set measuring period are split up by the beams splitters (ST1; ST2) arranged one after the other in the beam path of the light source (L). The random sequence is generated when the splitting up of the photons is matched with a predetermined photon model. The invention provides an inexpensive random-check generator which is easy to integrate onto a chip card, especially because of the light source (L) used.



(57) Zusammenfassung

Ziel der Erfindung ist ein kostengünstiges Verfahren und eine Anordnung zur Erzeugung binärer Sequenzen von Zufallszahlen. Die Lösung soll dabei so konzipiert werden, daß eine Integration auf eine Chipkarte in einfacher Art und Weise möglich ist. Das erfindungsgemäße Verfahren basiert auf dem Prinzip der zufälligen Wegwahl von Photonen an einem Strahlteiler und der Generierung einer Zufallszahl mittels zwei einem Strahlteiler (ST2) nachgeordneten Detektoren (D<sub>10</sub>; D<sub>21</sub>). Erfindungsgemäß wird zur Erzeugung von Photonen eine Lichtquelle (L) geringer Leistung verwendet und dem Strahlteiler (ST2) ein zusätzlicher Strahlteiler (ST1) vorgeschaltet. Die von der Lichtquelle (L) während einer vorgegebenen Meßzeit emittierten Photonen werden durch die nacheinander im Strahlengang der Lichtquelle (L) angeordneten Strahlteiler (ST1; ST2) aufgeteilt. Die Erzeugung der Zufallssequenz erfolgt bei Übereinstimmung der Aufteilung der Photonen mit einem vorher festgelegten Photonenschema. Die erfindungsgemäße Lösung stellt einen kostengünstigen Zufallsgenerator zur Verfügung, der sich insbesondere aufgrund der verwendeten Lichtquelle (L) in einfacher Art und Weise auf eine Chipkarte integrieren läßt.

# LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

|    |                              |    |                                      |    |  |    |                                   |
|----|------------------------------|----|--------------------------------------|----|--|----|-----------------------------------|
| AL | Albanien                     | ES | Spanien                              | LS | Lesotho  | SI | Slowenien                         |
| AM | Armenien                     | FI | Finnland                             | LT | Litauen  | SK | Slowakei                          |
| AT | Österreich                   | FR | Frankreich                           | LU | Luxemburg  | SN | Senegal                           |
| AU | Australien                   | GA | Gabun                                | LV | Lettland   | SZ | Swasiland                         |
| AZ | Aserbaidshan                 | GB | Vereinigtes Königreich               | MC | Monaco   | TD | Tschad                            |
| BA | Bosnien-Herzegowina          | GE | Georgien                             | MD | Republik Moldau                                    | TG | Togo                              |
| BB | Barbados                     | GH | Ghana                                | MG | Madagaskar   | TJ | Tadschikistan                     |
| BE | Belgien                      | GN | Guinea                               | MK | Die ehemalige jugoslawische<br>Republik Mazedonien | TM | Turkmenistan                      |
| BF | Burkina Faso                 | GR | Griechenland                         | ML | Mali   | TR | Türkei                            |
| BG | Bulgarien                    | HU | Ungarn                               | MN | Mongolei   | TT | Trinidad und Tobago               |
| BJ | Benin                        | IE | Irland                               | MR | Mauretanien  | UA | Ukraine                           |
| BR | Brasilien                    | IL | Israel                               | MW | Malawi   | UG | Uganda                            |
| BY | Belarus                      | IS | Island                               | MX | Mexiko   | US | Vereinigte Staaten von<br>Amerika |
| CA | Kanada                       | IT | Italien                              | NE | Niger  | UZ | Usbekistan                        |
| CF | Zentralafrikanische Republik | JP | Japan                                | NL | Niederlande  | VN | Vietnam                           |
| CG | Kongo                        | KE | Kenia                                | NO | Norwegen   | YU | Jugoslawien                       |
| CH | Schweiz                      | KG | Kirgisistan                          | NZ | Neuseeland   | ZW | Zimbabwe                          |
| CI | Côte d'Ivoire                | KP | Demokratische Volksrepublik<br>Korea | PL | Polen  |    |                                   |
| CM | Kamerun                      | KR | Republik Korea                       | PT | Portugal   |    |                                   |
| CN | China                        | KZ | Kasachstan                           | RO | Rumänien   |    |                                   |
| CU | Kuba                         | LC | St. Lucia                            | RU | Russische Föderation                               |    |                                   |
| CZ | Tschechische Republik        | LI | Liechtenstein                        | SD | Sudan  |    |                                   |
| DE | Deutschland                  | LK | Sri Lanka                            | SE | Schweden   |    |                                   |
| DK | Dänemark                     | LR | Liberia                              | SG | Singapur   |    |                                   |
| EE | Estland                      |    |                                      |    |  |    |                                   |

## **Verfahren und Anordnung zur Erzeugung binärer Sequenzen von Zufallszahlen**

### **Beschreibung:**

- 5 Die Erfindung betrifft ein Verfahren und eine Anordnung zur Erzeugung binärer Sequenzen von Zufallszahlen.

Zufallszahlen werden bei der mathematischen Simulation zufälliger Prozesse, bei der Stichprobenerhebung und besonders in der Kryptologie verwendet. Durch die zunehmend hochbitratige, digitale Kommunikation über öffentlich zugängliche Nach-

- 10 richtenkanäle ist die Gewährleistung der Geheimhaltung und der Authentizität der übertragenen Information zu einem zentralen Problem geworden. Gute kryptographische Schlüssel sind Sequenzen von binären Zufallszahlen. Zur sicheren Verschlüsselung wird vorzugsweise ein zufälliger Schlüssel dieser Art gewählt, der so lang wie die Nachricht selbst ist und nur ein einziges Mal Verwendung findet.

- 15 Zur Erzeugung von Zufallszahlen stehen im Wesentlichen zwei verschiedenartige Möglichkeiten zur Verfügung:

#### **1. durch mathematische Algorithmen generierte Pseudo-Zufallszahlen**

- Echte Zufallszahlen lassen sich in einem Rechner, der ja vollständig deterministisch  
20 arbeitet, grundsätzlich nicht erzeugen. Die durch mathematische Algorithmen generierten Zufallszahlen, die viele Programme zur Verfügung stellen, sind daher nie wirklich zu-fällig. Eine Verbesserung stellen die sogenannten Pseudozufallszahlen dar, die aus einem kürzeren echt zufälligen Keim entwickelt werden.

In jedem Fall ist jedoch bei der Generierung von Pseudozufallszahlen nach den o.g.

- 25 Verfahrensweisen mit einer gewissen Anzahl, von vorne herein unbrauchbarer Sequenzen (schwache Schlüssel) und auf jeden Fall mit seltsamen Korrelationen zu rechnen.

#### **2. Zufallszahlen, die auf physikalischen Verfahren basieren**

- Bei diesen Verfahren wird der statistische Charakter bestimmter physikalischer Prozesse  
30 genutzt.

Auch bei den physikalischen Verfahren gibt es solche, die zwar im Grunde deterministisch, aber dabei so komplex sind, daß sie nicht reproduziert werden können. Dazu gehören etwa der Münzwurf "Kopf" oder "Zahl", oder die Lottomaschinen. Diese Verfahren produzieren ein deterministisches Chaos, das als zufällig gelten kann, da die Anfangsbedingungen des Generators bei der Erzeugung jeder einzelnen Zufallszahl stets etwas voneinander abweichen, ohne daß diese Abweichung quantifizierbar wird.

Zu den physikalischen Verfahren gehören auch Elementarprozesse wie sie beispielsweise

in der Quantenmechanik vorkommen. Derartige Prozesse sind von ihrer Natur her grundsätzlich zufällig. Zufallszahlen, die durch physikalische Prozesse erzeugt werden, kommen daher dem Konzept einer zufälligen Sequenz näher als algorithmisch generierte Zufallszahlen.

Bekannt ist eine Lösung, die den natürlichen Quantenprozeß des elektromagnetischen Rauschens eines Widerstandes oder einer Diode zur Erzeugung von zufälligen Bitsequenzen nutzt (siehe Manfred Richter: Ein Rauschgenerator zur Gewinnung von quasi-idealen Zufallszahlen für die stochastische Simulation, Dissertation RWTH Aachen ; 1992).

Derartige Verfahren können jedoch von außen dadurch manipuliert werden, daß dem Quantenrauschen ein willkürlich vorgegebenes "Rauschen" etwa durch Einstrahlung elektromagnetischer Wellen überlagert wird. Da die Trennung des Quantenrauschens von diesem fremdbestimmten Pseudoruschen nicht einfach ist, gelten derartige Verfahren als nicht sicher.

Desweiteren sind Verfahren zur Generierung von Zufallszahlen bekannt, die auf radioaktiven Zerfallsprozessen basieren (siehe Martin Gude: „Ein quasi-idealer Gleichverteilungsgenerator basierend auf physikalischen Zufallsphänomenen“; Dissertation RWTH Aachen 1987). Dieses Verfahren eignet sich aufgrund der hohen Energie der entstehenden Teilchen sehr gut um Zufallssequenzen zu erzeugen, allerdings bestehen neben den wirklich vorhandenen Gefahren, die insbesondere auf der potentiell schädlichen Wirkung radioaktiver Strahlung auf den Menschen beruhen, bei einem Teil der

Bevölkerung irrationale Vorbehalte gegenüber der Radioaktivität, so daß radioaktive Prozesse nicht ohne weiteres zur Zufallserzeugung verwendet werden können.

Ein weiteres bekanntes Verfahren zur Erzeugung von Zufallssequenzen basiert auf dem  
5 Prozess der Wegwahl einzelner Photonen am Strahlteiler (siehe J.G. Rarity et al.: „Quantum random-number Generation and key sharing“ ; J. Mod. Opt. 41, S.2435 1994)

Bei diesem Verfahren wird ein Lichtquant z. B. an einem halbdurchlässigen Spiegel reflektiert oder transmittiert; zwei Detektoren registrieren das Lichtquant und ihre An-  
10 zeigen repräsentieren die "0" oder die "1" der Zufallssequenz.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren und eine Anordnung zur Erzeugung binärer Sequenzen von Zufallszahlen bereitzustellen, durch die die oben beschriebenen Nachteile vermieden werden. Die Lösung soll dabei kostengünstiger als die  
15 bekannten Lösungen sein und sich ohne großen Aufwand auf eine Chipkarte integrieren lassen.

Die Aufgabe wird erfindungsgemäß durch die kennzeichnenden Merkmale des 1. Patentanspruchs gelöst. Vorteilhafte Ausgestaltungen und Weiterbildungen ergeben sich aus den Unteransprüchen.

20 Die erfindungsgemäße Lösung basiert auf dem bekannten Prinzip der Wegwahl einzelner Photonen an einem Strahlteiler. Bei der erfindungsgemäßen Lösung wird ein optischer Strahlteiler, z. B. ein halbdurchlässiger Spiegel verwendet, auf den ultraviolette, sichtbares oder infrarotes Licht fällt. Zwei Detektoren, die einzelne Photonen erkennen können, registrieren die Photonen und definieren über die ihnen zugeordneten Anzeigen  
25 die „0“ oder die „1“ der Zufallssequenz und damit die Zufallsfolge.

Bei dem erfindungsgemäßen Verfahren wird als Lichtquelle L anstatt der bisher üblichen Photonenquelle, wie beispielsweise eine abgeschwächte Laserstrahlquelle, eine Photonenquelle geringerer Leistung und damit auch geringerer Abmessung eingesetzt. Geeignet sind beispielsweise abgeschwächte Laserdioden, normale Dioden (LEDs),  
30 thermische Lichtquellen wie Halogenlampen, Spektrallampen oder Quetschlichtquellen. Desweiteren wurde erfindungsgemäß vor dem zweiten Strahlteiler ST2 ein erster

Strahlteiler ST1, vorzugsweise ein Triggerstrahlteiler, in den Strahlgang der Lichtquelle L eingefügt. Die entsprechend dem Zufallsprinzip von der Lichtquelle L während einer vorgegebenen Meßzeit emittierten Photonen/Photonenschwärme werden dabei durch die im Strahlgang der Lichtquelle L angeordneten Strahlteiler ST1 und ST2 auf-  
5 geteilt und entsprechend der Aufteilung über die den Strahlteilern ST1 und ST2 nachgeordneten Detektoren (Triggerdetektor DT für Strahlteiler ST1 und die Detektoren D1<sub>0</sub> und D2<sub>1</sub> für den Strahlteiler ST2) erfaßt.

Die Detektoren DT, D1<sub>0</sub> und D2<sub>1</sub> sind mit der Erfassungseinrichtung E verbunden.,

Eine Zufallszahl wird nur erzeugt, wenn die an den einzelnen Detektoren DT, D1<sub>0</sub> und  
10 D2<sub>1</sub> registrierten Photonen in ihrer Gesamtheit einem vorher festgelegten Photonenzahlschema entsprechen, welches in den Rechner der Erfassungseinrichtung eingegeben wurde.

Die mathematischen Grundlagen sowie die möglichen Ausführungsformen der erfindungsgemäßen Lösung werden nachfolgend anhand von Figur 1 näher erläutert.

15

Als Lichtquelle L wird eine Lichtquelle gewählt, bei der Lichtintensität derart schwach ausgebildet ist, daß sie einzelne Photonen oder aber stets mit einer gewissen Wahrscheinlichkeit auch Photonenschwärme aus n Photonen aussendet. Diese Photonen-  
schwärme werden dann in den Detektoren DT, D1<sub>0</sub> und D2<sub>1</sub> entweder aufgelöst oder als  
20 ganzes als Einzelergebnis gezählt. Die Wahrscheinlichkeit p<sub>n</sub>, daß am Detektor gleichzeitig n Photonen auftreten oder als Einzelereignis gezählt werden, wird durch die Poissonverteilung beschrieben.

$$p_n = \frac{\bar{n}^n}{n!} e^{-\bar{n}} \quad (1)$$

25

$\bar{n}$  ist die mittlere Zahl der Photonen pro Meßzeit am Detektor. Obwohl die Statistik der Lichtquelle für thermisches Licht (Halogenlampe), chaotisches Licht (Spektrallinie) oder Laserlicht verschieden ist, gilt Gleichung (1) für alle diese Lichtquellen, solange die Kohärenzzeit einer thermischen oder chaotischen Quelle kurz im Vergleich zu Meß-  
30 zeit des Detektors ist. Für Laserlicht gilt immer die Gleichung (1). Beim einfachen

Strahlteiler mit zwei Detektoren, wie er durch den Strahlteiler ST2 und die Detektoren D1<sub>0</sub> und D2<sub>1</sub> in Fig. 1 abgebildet ist, wird die Elektronik der Zählvorgänge so eingerichtet, daß ein Ergebnis immer nur dann gezählt wird, wenn nur einer der Detektoren D1<sub>0</sub> oder D2<sub>1</sub> anspricht. Sprechen beide Detektoren D1<sub>0</sub> und D2<sub>1</sub> innerhalb der Meßzeit an, so wird das Zählereignis verworfen. Wird ein Schwarm von Photonen am Strahlteiler ST2 aufgeteilt, so wird das Ereignis nicht gewertet. Gewertet wird ein Zählereignis nur, wenn der Schwarm völlig in den einen Detektor D1<sub>0</sub> oder völlig in den anderen Detektor D2<sub>1</sub> gelangt und gezählt wird. Bei einem Schwarm von n Photonen bedeutet dies, daß nur 2 von n+1 Ereignissen gezählt werden, und Gleichung (1) ist daher noch

mit  $\frac{2}{n+1}$  zu multiplizieren, um die Wahrscheinlichkeit zu beschreiben, mit der Zählereignisse bei einem Photonenschwarm auftreten. Also:

Die Wahrscheinlichkeit  $p_n$ , daß bei einer mittleren Photonenzahl  $\bar{n}$  ein brauchbares Zählereignis auftritt, beträgt für den einfachen Strahlteiler, entsprechend Strahlteiler ST2, und einer der oben beschriebenen Lichtquellen L geringer Leistung

$$p_n^{(1)} = \frac{\bar{n}^n}{n!} e^{-\bar{n}} \cdot \frac{2}{n+1} \quad \text{einfacher Strahlteiler} \quad (2)$$

Erfindungsgemäß wird dem einfachen Strahlteiler ST2 ein weiterer Strahlteiler ST1, vorzugsweise ein Triggerstrahlteiler, vorschaltet (Fig.1). Wie im ersten Fall sind die Zähl-  
elektroniken der beiden Detektoren D1<sub>0</sub> und D2<sub>1</sub> so geschaltet, daß eine Zufallszahl nur dann bestimmt wird, wenn nur der eine oder nur der andere Detektor D1<sub>0</sub> oder D2<sub>1</sub> anspricht. Außerdem darf in diesem Fall aber der Triggerdetektor DT des Strahlteilers ST1 nicht ansprechen. Laufzeiteffekte zwischen dem Triggerdetektor DT des ersten Strahlteilers ST1 und den Detektoren D1<sub>0</sub> und D2<sub>1</sub> des zweiten Strahlteiler ST2 werden optisch oder elektronisch ausgeglichen. Tritt ein Schwarm von n Photonen auf, und gelangt wenigstens 1 Photon des Schwarmes in den Triggerdetektor DT, wird das Ereignis nicht gezählt. Nur wenn kein Photon über den ersten Strahlteiler ST1 zum Triggerdetektor DT gelangt und außerdem am zweiten Strahlteiler ST2 alle n Photonen vollständig, entweder in den Detektor D1<sub>0</sub>, oder in den Detektor D2<sub>1</sub> gelangen, wird ein Er-

gebnis als (0) oder (1) gezählt. Die Wahrscheinlichkeit, daß kein Photon des Schwar-  
mes zum Triggerdetektor DT gelangt und der Rest völlig zu einem der Detektoren D1<sub>0</sub>  
oder D2<sub>1</sub>, beträgt  $4/((n+1)(n+2))$ , d. h. die Wahrscheinlichkeit  
 $p_n^{(2)}$ , daß bei einem Schwarm von n Photonen ein Zählereignis auftritt, beträgt

5

$$p_n^{(2)} = \frac{\bar{n}^n}{n!} e^{-\bar{n}} \cdot \frac{4}{(n+1)(n+2)} \quad \text{Strahlteiler ST2 mit vorgeschaltetem} \quad (3)$$

Strahlteiler ST1

Die Gleichung (3) gilt für den Fall, daß der Strahlteiler ST1 das Teilungsverhältnis  
10  $1/3 : 2/3$ , der Strahlteiler ST2 aber das Teilungsverhältnis  $1/2 : 1/2$  hat. In diesem Fall  
werden die drei Detektoren DT; D1<sub>0</sub>; D2<sub>1</sub> gleich gewichtet. Andere Teilungsverhältnisse  
sind möglich, verändern aber die Wahrscheinlichkeiten nach Gleichung (3).

Das hier angewendete Verfahren macht es also mit zunehmender Anzahl n der während  
15 einer vorgegebenen Meßzeit emittierten Photonen immer unwahrscheinlicher, daß ein  
n-Photonenschwarm zu einem Zählereignis und damit zu einer Zufallszahl führt. Aber  
die Wahrscheinlichkeit nimmt zu, daß der quantenmechanisch ideale Fall eintritt: näm-  
lich die Erzeugung des Zufalls durch ein einzelnes Photon am Strahlteiler. Die Mehr-  
photonen-

20 ereignisse, die im Grenzfall großer n in den klassischen Zustand übergehen, werden  
unterdrückt. Damit können erfindungsgemäß schwache Laser, chaotische oder thermi-  
sche Lichtquellen zur Zufallserzeugung herangezogen werden.

Denkbar ist auch die Anordnung von mehr als einem Triggerstrahlteiler, in den Strahl-  
gang zwischen Lichtquelle L und Strahlteiler ST2. Die Triggerdetektoren dieser zu-  
25 sätzlichen Triggerstrahlteiler sind ebenfalls mit der Erfassungseinrichtung E verbunden.  
Bei einer derartigen Ausführungsform werden die während der vorgegeben Meßzeit  
detektierten Photonen, entsprechend ihrer Zuordnung zu den einzelnen Triggerstrahl-  
teilern (einschließlich Strahlteiler ST2), in der Erfassungseinrichtung registriert und eben-  
falls mit einem vorher festgelegten, in der Erfassungseinrichtung E gespeicherten Pho-  
30 tonenschema verglichen. Bei einer solchen Ausführungsform werden Photonenschwär-

me noch stärker unterdrückt. Zufallsereignisse werden beispielsweise nur registriert, wenn keiner der Triggerdetektoren anspricht.

Auch ein anderes festgelegtes oder variabel veränderbares Photonenschema kann bei einer Ausführungsform mit mehreren Triggerdetektoren im Strahlgang der Lichtquelle

5 L vorgegeben werden. Das Photonenschema kann beispielsweise beinhalten, daß der Triggerdetektor jedes zweiten Triggerstrahlteilers ansprechen muß, oder daß nur der Triggerdetektor des ersten und des siebten Triggerstrahlteilers ansprechen muß. In jedem dieser Fälle wird die Zählwahrscheinlichkeit für den Photonenschwarm vermindert.

10 Ein interessantes Beispiel ist eine Anordnung nach Fig.1, bei der Zufallsereignisse am zweiten Strahlteiler ST2 nur gezählt werden, wenn ein oder mehrere Photonen durch den Triggerdetektor DT des Strahlteilers ST1 registriert werden. In diesem Fall werden Schwärme mit nur einem Photon gar nicht für die Zufallserzeugung verwendet. Da die heutigen Detektoren auch recht unangenehme Eigenschaften, wie geringe Quanteneffizienz und Totzeiten haben, handelt man sich mit weiteren zusätzlichen Triggerstrahlteilern auch zusätzliche elektronische Schwierigkeiten und Kosten ein. In der Praxis wird  
15 also vorzugsweise nur ein zusätzlicher Triggerstrahlteiler eingesetzt werden.

20

25

30

**Bezugszeichenaufstellung:**

|    |                   |  |
|----|-------------------|--|
|    | L                 | Lichtquelle  |
|    | ST1               | erster Strahlteiler (Triggerstrahlteiler)                      |
| 5  | ST2               | zweiter Strahlteiler   |
|    | E                 | Erfassungseinrichtung  |
|    | DT                | Triggerdetektor des ersten Strahlteilers                       |
|    | D1 <sub>0</sub> I |  |
| 10 | I                 | Detektoren des zweiten Strahlteilers                           |
|    | D2 <sub>1</sub> I |  |
|    | n                 | Anzahl der während einer vorgegebenen Meßzeit durch die Licht- |
|    | quelle            | emittierten Photonen   |

## Verfahren und Anordnung zur Erzeugung binärer Sequenzen von Zufallszahlen

### (10) Patentansprüche

- 5 1. Verfahren zur Erzeugung binärer Sequenzen von Zufallszahlen, welches auf dem Prinzip der zufälligen Wegwahl von Photonen an einem Strahlteiler und der Generierung einer Zufallszahl mittels zwei einem Strahlteiler nachgeordneten Detektoren beruht, und bei dem die Zählerlektroniken der beiden Detektoren so geschaltet sind, daß eine Zufallszahl dann generiert wird, wenn nur einer der Detektoren an-  
10 spricht, **d a d u r c h g e k e n n z e i c h n e t**,  
daß die von einer als Lichtquelle (L) geringer Leistung ausgebildeten Photonenquelle entsprechend dem Zufallsprinzip während einer vorgegebenen Meßzeit emittierten Photonen/Photonenschwärme durch mindestens zwei nacheinander im Strahlgang der Lichtquelle (L) angeordnete Strahlteiler (ST1;ST2) aufgeteilt und  
15 entsprechend der Aufteilung über die den Strahlteilern (ST1;ST2) nachgeordneten, mit der Erfassungseinrichtung (E) verbundenen Detektoren (DT;D1<sub>0</sub>,D2<sub>1</sub>) erfaßt werden, und daß eine Zufallszahl nur erzeugt wird, wenn die an den einzelnen Detektoren (DT;D1<sub>0</sub>,D2<sub>1</sub>) registrierten Photonen in ihrer Gesamtheit einem vorher festgelegten Photonenschema entsprechen.  
20
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß bei zwei nacheinander im Strahlgang der Lichtquelle (L) angeordneten Strahlteilern (ST1;ST2) das der Erzeugung der Zufallszahl zugrunde liegende Photonenzahlschema darauf beruht, daß eine Zufallszahl nur erzeugt wird, wenn während der vorgegebenen Meßzeit  
25 am Triggerdetektor (DT) des ersten Strahlteilers (ST1) kein Photon und nur an einem der dem zweiten Strahlteiler (ST2) nachgeordneten Detektoren (D1<sub>0</sub>) bzw. (D2<sub>1</sub>) mindestens ein Photon registriert wird.
3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß bei zwei nacheinander im  
30 Strahlgang der Lichtquelle angeordneten Strahlteilern (ST1;ST2) das der Erzeugung der Zufallszahl zugrunde liegende Photonenzahlschema darauf beruht, daß ei-

ne Zufallszahl nur erzeugt wird, wenn während der vorgegebenen Meßzeit am Detektor (DT) des ersten Strahlteilers (ST1) mindestens ein Photon und nur an einem der dem zweiten Strahlteiler (ST2) nachgeordneten zwei Detektoren (D1<sub>0</sub>) bzw. (D2<sub>1</sub>) mindestens ein Photon registriert wird.

5

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß für den Fall, daß mehr als zwei Triggerstrahlteiler im Strahlgang zwischen der Lichtquelle (L) und dem Strahlteiler (ST2) angeordnet sind, das Photonenschema mathematisch so ausgebildet ist, daß eine Zufallszahl nur erzeugt wird, wenn ein Photonenschwarm mit einer durch das vorgegebene Photonenschema definierten Anzahl von Photonen an den Detektoren des Strahlteilers (ST2) und den Triggerdetektoren der zusätzlichen Triggerstrahlteiler auftritt.

10

5. Anordnung zur Erzeugung binärer Sequenzen von Zufallszahlen, umfassend
- eine als Photonenquelle ausgebildete Lichtquelle,
  - einen der Lichtquelle nachgeordneten Strahlteiler mit zwei dem Strahlteiler nachgeordneten Detektoren und
  - eine den Detektoren nachgeordnete, aus Zähler und Rechner bestehende Erfassungseinrichtung zur Generierung der Zufallszahlen,

15

**dadurch gekennzeichnet**, daß als Photonenquelle eine Lichtquelle (L) geringer Leistung eingesetzt wird, aus der entsprechend dem Zufallsprinzip sowohl einzelne Photonen als auch Photonenschwärme austreten können, und daß zwischen der Lichtquelle (L) und dem im Strahlgang der Lichtquelle (L) angeordnetem Strahlteiler (ST2) mindestens ein weiterer Strahlteiler, vorzugsweise ein Triggerstrahlteiler (ST1), im Strahlgang angeordnet ist, welcher über einen Detektor, vorzugsweise einen Triggerdetektor (DT), mit der Erfassungseinrichtung (E) verbunden ist.

20

25

6. Anordnung nach Anspruch 5, dadurch gekennzeichnet, daß als Lichtquelle (L) ein abgeschwächter Laser verwendet wird.

30

7. Anordnung nach Anspruch 5, dadurch gekennzeichnet, daß als Lichtquelle (L) eine thermische Lichtquelle verwendet wird.

5 8. Anordnung nach Anspruch 5, dadurch gekennzeichnet, daß als Lichtquelle (L) eine Spektrallampe verwendet wird.

9. Anordnung nach Anspruch 5, dadurch gekennzeichnet, daß als Lichtquelle (L) eine Leuchtdiode verwendet wird.

10 10. Anordnung nach Anspruch 4, dadurch gekennzeichnet, daß als Lichtquelle (L) eine Quetschlichtquelle verwendet wird.

15

20

25

30

**THIS PAGE BLANK (USPTO)**

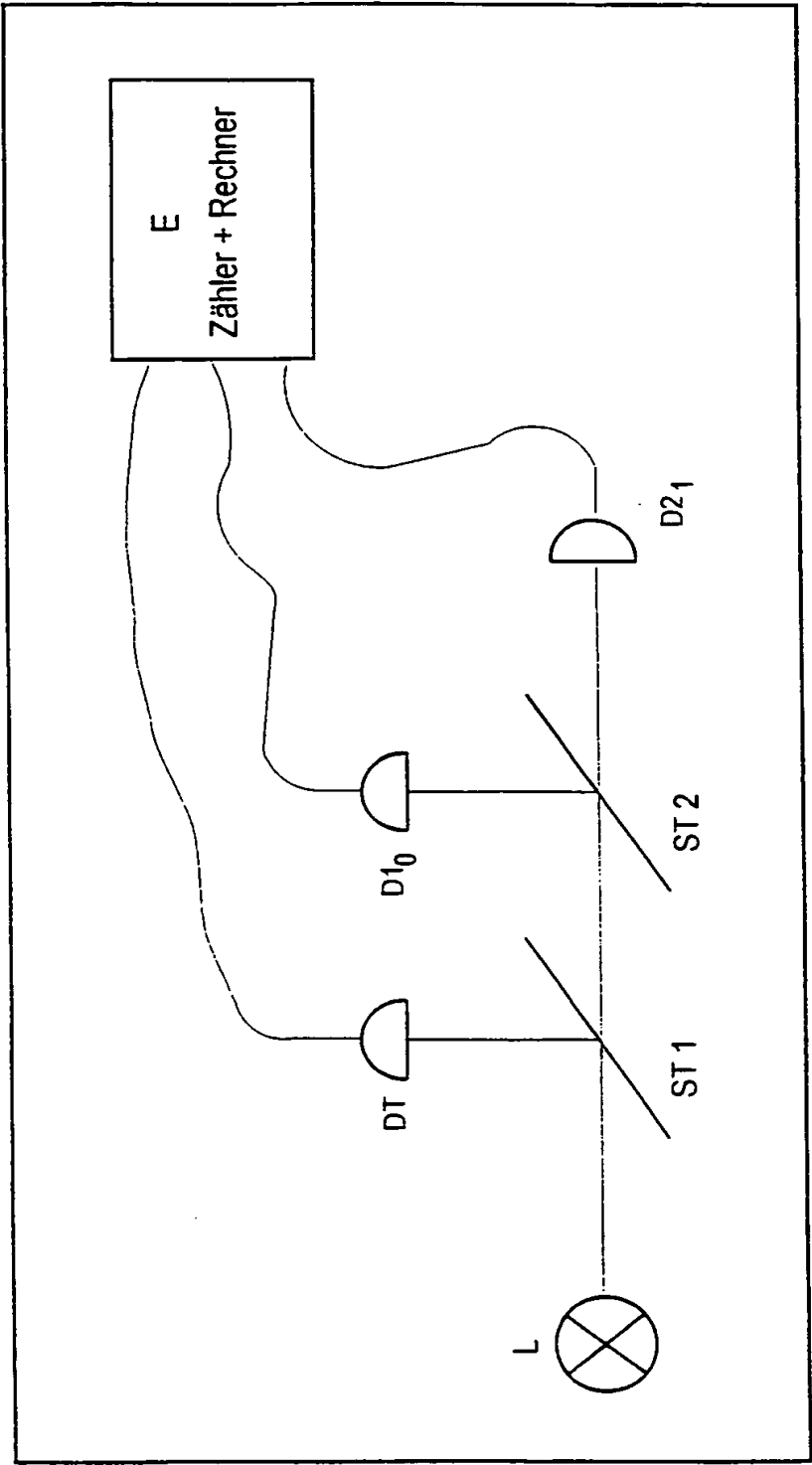


Fig. 1



**THIS PAGE BLANK (USPTO)**

# INTERNATIONAL SEARCH REPORT

International Application No.

PCT/EP 98/08057

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 6 H03K3/84

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G06F H03K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category * | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
|------------|--|-----------------------|
| A          | RARITY J G ET AL: "QUANTUM RANDOM-NUMBER GENERATION AND KEY SHARING"<br>JOURNAL OF MODERN OPTICS,<br>vol. 41, no. 12, December 1994, pages<br>2435-2444, XP002052913<br>cited in the application<br>see the whole document | 1,5                   |
| A          | US 4 687 935 A (NURMI JARMO ET AL)<br>18 August 1987<br>see abstract   | 1,5                   |
| A          | TAKEUCHI S ET AL: "HIGH PERFORMANCE RANDOM PULSER BASED ON PHOTON COUNTING"<br>IEEE TRANSACTIONS ON NUCLEAR SCIENCE,<br>vol. NS-33, no. 1, February 1986, pages<br>946-949, XP002022448<br>see page 946                    | 1,5                   |
| -/--       |  |                       |

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

26 March 1999

Date of mailing of the international search report

12/04/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Verhoof, P

# INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 98/08057

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
|----------|--|-----------------------|
| A        | <p>           DATABASE INSPEC<br/>           INSTITUTE OF ELECTRICAL ENGINEERS,<br/>           STEVENAGE, GB<br/>           Inspec No. 3095523,<br/>           TANG QING ET AL: "Monte Carlo calculation<br/>           for random numbers produced by an optical<br/>           method"<br/>           XP002098144<br/>           see abstract<br/>           &amp; WULI, JUNE 1987, CHINA,<br/>           vol. 16, no. 6, pages 349-352,<br/>           ISSN 0379-4148<br/>           -----         </p> | 1,5                   |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 98/08057

| Patent document<br>cited in search report | Publication<br>date | Patent family<br>member(s) | Publication<br>date |
|---|---------------------|----------------------------|---------------------|
| US 4687935 A                              | 18-08-1987          | SE 445495 B                | 23-06-1986          |
|   |                     | DE 3565320 A               | 03-11-1988          |
|   |                     | EP 0181302 A               | 14-05-1986          |
|   |                     | JP 61118682 A              | 05-06-1986          |
|   |                     | SE 8405620 A               | 10-05-1986          |
| <hr/>                                     |                     |                            |                     |

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 98/08057

## A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 6 H03K3/84

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

## B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 6 G06F H03K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

## C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile   | Betr. Anspruch Nr. |
|------------|--|--------------------|
| A          | RARITY J G ET AL: "QUANTUM RANDOM-NUMBER GENERATION AND KEY SHARING"<br>JOURNAL OF MODERN OPTICS,<br>Bd. 41, Nr. 12, Dezember 1994, Seiten<br>2435-2444, XP002052913<br>in der Anmeldung erwähnt<br>siehe das ganze Dokument | 1,5                |
| A          | US 4 687 935 A (NURMI JARMO ET AL)<br>18. August 1987<br>siehe Zusammenfassung   | 1,5                |
| A          | TAKEUCHI S ET AL: "HIGH PERFORMANCE RANDOM PULSER BASED ON PHOTON COUNTING"<br>IEEE TRANSACTIONS ON NUCLEAR SCIENCE,<br>Bd. NS-33, Nr. 1, Februar 1986, Seiten<br>946-949, XP002022448<br>siehe Seite 946                    | 1,5                |

---  
-/--

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

\* Besondere Kategorien von angegebenen Veröffentlichungen:

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung: die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung: die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

26. März 1999

Absendedatum des internationalen Recherchenberichts

12/04/1999

Name und Postanschrift der Internationalen Recherchenbehörde  
Europäisches Patentamt, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Verhoof, P

| C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN |  |                    |
|--|--|--------------------|
| Kategorie  | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile   | Betr. Anspruch Nr. |
| A  | <p>DATABASE INSPEC<br/>INSTITUTE OF ELECTRICAL ENGINEERS,<br/>STEVENAGE, GB<br/>Inspec No. 3095523,<br/>TANG QING ET AL: "Monte Carlo calculation<br/>for random numbers produced by an optical<br/>method"<br/>XP002098144<br/>siehe Zusammenfassung<br/>&amp; WULI, JUNE 1987, CHINA,<br/>Bd. 16, Nr. 6, Seiten 349-352,<br/>ISSN 0379-4148</p> <p>-----</p> | 1,5                |

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 98/08057

| Im Recherchenbericht<br>angeführtes Patentdokument | Datum der<br>Veröffentlichung | Mitglied(er) der<br>Patentfamilie | Datum der<br>Veröffentlichung |
|--|-------------------------------|-----------------------------------|-------------------------------|
| US 4687935 A                                       | 18-08-1987                    | SE 445495 B                       | 23-06-1986                    |
|  |                               | DE 3565320 A                      | 03-11-1988                    |
|  |                               | EP 0181302 A                      | 14-05-1986                    |
|  |                               | JP 61118682 A                     | 05-06-1986                    |
|  |                               | SE 8405620 A                      | 10-05-1986                    |
| <hr/>  |                               |                                   |                               |